UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/707,100	11/20/2003	Troy Rockwood	03-0049	1099

64722 7590 05/02/2008

OSTRAGER CHONG FLAHERTY & BROITMAN, P.C.
570 LEXINGTON AVENUE
FLOOR 17
NEW YORK, NY 10022-6894

EXAMINER	
DOAN, TRANG T	

ART UNIT	PAPER NUMBER
2131	

NOTIFICATION DATE	DELIVERY MODE
05/02/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JBROITMAN@OCFBLAW.COM
lmurrell@ocfblaw.com
patentadmin@boeing.com

Office Action Summary	Application No.	Applicant(s)	
	10/707,100	ROCKWOOD ET AL.	
	Examiner	Art Unit	
	TRANG DOAN	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment filed on 02/05/2008.

2. Claims 1-38 are pending for consideration.

Response to Arguments

3. Applicant's arguments filed on 02/05/2008 have been fully considered but they are not persuasive.

Applicant's argument, on page 3 of the Remarks, that Leo does not teach a distributed authentication infrastructure wherein, as claimed in the present invention, each of the nodes can authenticate the plurality of the nodes. Examiner respectfully disagrees with Applicant's argument. Leo does teach the distributed authentication infrastructure, each of the nodes can authenticate the plurality of the nodes (Leo: See figure 1 items [10, 12 and 14] and paragraphs 0035, 0068, 0070, 0074, 0078-0079, 0082-0087: client unit stores a digital certificate which shares among a plurality of client units. The digital certificate is used by each client to authenticate each other). According to the above cited portions, Examiner interprets the client unit, the corporate server and the secure bridging unit as the distributed authentication infrastructure because each node can authenticate with each other nodes.

Applicant's argument, on page 3 of the Remarks, that Leo does not teach the sequence (implementation of distributed authentication infrastructure followed by implementation of centralized authentication structure). Examiner respectfully disagrees with Applicant's argument. Leo does teach the sequence (implementation of

distributed authentication infrastructure followed by implementation of centralized authentication structure) (Leo: See Abstract section: "a central management unit manages the plurality of client units, the corporate server and the secure bridging unit" and paragraphs 0077, 0089-0090 and 0127). According the cited portions above, the client unit, the corporate server and the secure bridging unit, need to set up first in order for them to authenticate with each other. After the set up step, the central management server controls the communication between them, therefore Leo does teach the sequence (Leo: paragraph 0051: the central management server manages multiple databases which comprise userid and password of the client unit, the corporate server and the secure bridging unit).

The Applicant argues that Leo in view of Dinker fails to teach wherein said distributed authentication infrastructure requires a quorum of said plurality of nodes for enrolling a new entity into the hybrid authentication system. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413,208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091,231 USPQ 375 (Fed. Cir. 1986).

The Applicant argues that Leo in view of Prabandham fails to teach producing a log for recording a plurality of failed authentications and a plurality of failed enrollments by said plurality of nodes. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642

F.2d 413,208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091,231 USPQ 375 (Fed. Cir. 1986).

The Applicant argues that Leo in view of Benatar fails to teach each node of said quorum utilizes a partial key for partially signing a certificate related to said new entity so as to provide said new entity with a full signature. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413,208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091,231 USPQ 375 (Fed. Cir. 1986).

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that cited prior arts do teach or suggest the subject matter broadly recited in independent claims 1, 23-24 and 29, and in subsequent dependent claims. Accordingly, rejections for claims 1-38 are respectfully maintained.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-3, 7, 11, 13-14, 18, 22-24, 29-34 and 36 are rejected under 35 U.S.C. 102(e) as being anticipated by Leoutsarakos (US 2004/0039905) (hereinafter Leo).

Regarding claim 1, Leo discloses a distributed authentication infrastructure including a plurality of nodes in communication with each other, each of said plurality of nodes having an identification and intended to perform a series of functions, one of said series of functions for verifying said identification of said plurality of nodes (Leo: see figures 1, figure 7 (e.g., client unit 1 and corporate server are two distributed nodes) and paragraph 0074); and a centralized authentication infrastructure integrated into said distributed authentication infrastructure and including a central server, said central server being coupled to said plurality of nodes and being utilized for verifying said identification of said plurality of nodes (Leo: see Abstract section and paragraphs 0011, 0051 (a central management unit manages a plurality of client units, a corporate server and a secure bridging unit)); wherein said distributed authentication infrastructure is initially implemented and said centralized authentication infrastructure is later integrated into said distributed authenticated infrastructure (Leo: see figure 1 (a central management server controls the communications among a plurality of clients, corporate server and secure bridging unit)); wherein said distributed authentication infrastructure is selected from the group consisting of a threshold cryptography service model and a

web-of-trust service model (Leo: paragraphs 0057, 0061, 0064, 0072, 0085, 0096, 0108 and 0110); wherein said centralized authentication system is selected from the group consisting of a public key infrastructure and a Kerberos service model (Leo: paragraphs 0035 and 0057); wherein said plurality of nodes include at least one of a personal digital assistant, a digital pager, a digital fax machine, a vide teleconferencing device, a wireless telephone, a portable computer, a desktop computer, and a communication device (Leo: paragraphs 0029 and 0034).

Regarding claims 2 and 36, Leo further discloses wherein said plurality of nodes includes a verifying node coupled to a new entity for verifying the identification of said new entity and enrolling said new entity into the hybrid authentication system (Leo: paragraph 0122).

Regarding claim 3, Leo further discloses wherein said new entity provides said verifying node with at least one predetermined credential (Leo: paragraph 0122).

Regarding claims 7 and 11, Leo further discloses wherein said central server is said new entity (Leo: see figure 1 item 16).

Regarding claim 13, Leo further discloses wherein said central server is coupled to said plurality of nodes for at least one of issuing a global directive thereto and bolstering said plurality of nodes by assisting with at least one of an enrollment task, an authentication task, and a permission granting task (Leo: see figure 1 item 16 and paragraphs 0013, 0051, 0120 and 0122).

Regarding claims 14 and 31, Leo further discloses wherein said global directive includes at least one of a rekey instruction and a critical trust chain path, said rekey

instruction and said critical trust chain path for providing a secured data transfer line (Leo: paragraphs 0011 and 0118 (e.g., re-generate all session keys and secure bridging unit)).

Regarding claims 18 and 22, Leo further discloses wherein said second node is coupled to a trusted third party node from said plurality of nodes, said second node producing an authentication task signed by said first node and sending said authentication task to said trusted third party node, said trusted third party node verifying said identification of said first node (Leo: see figure 1 and Abstract section).

Regarding claim 23, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Regarding claim 24, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Regarding claim 29, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Regarding claim 30, Leo further discloses wherein said central server is coupled to said plurality of nodes for at least one of issuing a global directive thereto and supporting said plurality of nodes by assisting with at least one of an enrollment task, an authentication task, and a permission granting task (Leo: see figure 1, Abstract section and paragraphs 0013 and 0120-0122).

Regarding claim 32, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Regarding claim 33, Leo further discloses wherein migrating comprises coupling a central server to said plurality of nodes (Leo: see figure 1).

Regarding claim 34, Leo further discloses coupling said central server to a verifying node of said plurality of nodes; sending at least one predetermined credential from said central server to said verifying node; enrolling said central server into the hybrid authentication system (Leo: see figure 1 and paragraphs 0013 and 0122).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 8 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leo in view of Dinker (US 20040254984) (hereinafter Dinker).

Regarding claim 8, Leo does not disclose wherein said distributed authentication infrastructure requires a quorum of said plurality of nodes for enrolling a new entity into the hybrid authentication system. However, Dinker discloses the quorum of said plurality of nodes for enrolling a new entity (Dinker: see figure 3 and paragraph 0010). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of the quorum method of Dinker into the system of Leo to enhance security because the pre-selected nodes have to vote and agree with each other in order for the new entity get enrolled into the system.

Regarding claim 38, this claim has limitations that is similar to those of claim 8, thus it is rejected with the same rationale applied against claim 8 above.

8. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Leo in view of Prabandham et al. (US 6701438) (hereinafter Prahandham).

Regarding claim 12, Leo does not disclose in details wherein said central server is coupled to a new entity and is utilized for verifying the identification of said new entity and enrolling said new entity into the hybrid authentication system, said central server producing a log for recording a plurality of failed authentications and a plurality of failed enrollments by said plurality of nodes. However, Prabandham discloses logging all failed authentications and/or failed authorizations by logging module (Prabandham: see figure 2 and column 3 line 65 through column 4 line 1). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of logging all failed authentications and/or authorization of Prahandham into the system of Leo because logging module provides the selected logging protocols such that those received requests that do not have originate from the verified source or do not have appropriate permission are recorded by the logging module (Prabandham: column 2 lines 49-52)

9. Claims 4-6, 15-17, 19-21, 25-28, 35 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable Leo in view of Benantar (US 2003/0130947) (hereinafter Ben).

Regarding claim 4, Leo does not explicit disclose wherein said verifying node signs a certificate related to said new entity. However, Ben discloses wherein said verifying node signs a certificate related to said new entity (Ben: column 1 paragraph [0012]). Therefore, it would have been obvious to one ordinary skill in the art to apply

the teaching of the certificate of Ben into the method of Leo to have a method and system that simplifies the administrative processing associated with the trust paths that are required for valid use of digital certificates (Ben: paragraph [0011]).

Regarding claims 5, 17 and 20, Leo does not explicit disclose wherein said central server publishes a certificate revocation list, said verifying node examining said certificate revocation list for determining whether said certificate has been revoked. Ben discloses wherein said central server publishes a certificate revocation list, said verifying node examining said certificate revocation list for determining whether said certificate has been revoked (Ben: paragraphs [0043, 0047 and 0057]). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of the certificate revocation list of Ben into the method of Leo to have a method and system that simplifies the administrative processing associated with the trust paths that are required for valid use of digital certificates (Ben: paragraph [0011]).

Regarding claims 6, 16 and 21, Leo does not explicit disclose wherein a quorum of said plurality of nodes publishes a certificate revocation list, said verifying node examining said certificate revocation list for determining whether said certificate has been revoked. Ben discloses wherein a quorum of said plurality of nodes publishes a certificate revocation list, said verifying node examining said certificate revocation list for determining whether said certificate has been revoked (Ben: paragraphs [0043, 0047 and 0057]). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of the certificate revocation list of Ben into the method of Leo to have

a method and system that simplifies the administrative processing associated with the trust paths that are required for valid use of digital certificates (Ben: paragraph [0011]).

Regarding claims 15 and 19, Leo does not explicit disclose wherein said plurality of nodes includes a first node and a second node coupled to said first node, said first node presenting a first certificate to said second node for authenticating said first node. Ben discloses wherein said plurality of nodes includes a first node and a second node coupled to said first node, said first node presenting a first certificate to said second node for authenticating said first node (Ben: paragraphs [0008 and 0045]). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of using a certificate of Ben into the method of Leo to have a method and system that simplifies the administrative processing associated with the trust paths that are required for valid use of digital certificates (Ben: paragraph [0011]).

Regarding claims 25-27, Leo does not explicit disclose wherein said plurality of nodes is a plurality of members including a first member and a second member, said certificate authority issuing a first group certificate to said first member that provides said first member with a first permission level, said certificate authority issuing a second group certificate to said second member that provides said second member with a second permission level. Ben discloses wherein said plurality of nodes is a plurality of members including a first member and a second member, said certificate authority issuing a first group certificate to said first member that provides said first member with a first permission level, said certificate authority issuing a second group certificate to said second member that provides said second member with a second permission level

(Ben: see Abstract section). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of using a certificate of Ben into the method of Leo to have a method and system that simplifies the administrative processing associated with the trust paths that are required for valid use of digital certificates (Ben: paragraph [0011]).

Regarding claim 28, this claim has limitations that are similar to those of claims 25-27, thus it is rejected with the same rationale applied against claims 25-27 above.

Regarding claims 35 and 37, Leo does not explicit disclose coupling said central server to a verifying node of said plurality of nodes; sending a certificate revocation list from said central server to said verifying node; enrolling said central server into the hybrid authentication system. Ben discloses coupling said central server to a verifying node of said plurality of nodes; sending a certificate revocation list from said central server to said verifying node; enrolling said central server into the hybrid authentication system (Ben: see Abstract section and paragraph [0043]). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of using a certificate of Ben into the method of Leo to have a method and system that simplifies the administrative processing associated with the trust paths that are required for valid use of digital certificates (Ben: paragraph [0011]).

10. Claims 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leo in view of Dinker, and further in view of Ben.

Regarding claim 9, Leo does not explicit disclose wherein each node of said quorum utilizes a partial key for partially signing a certificate related to said new entity

so as to provide said new entity with a full signature. Ben discloses wherein each node of said quorum utilizes a partial key for partially signing a certificate related to said new entity so as to provide said new entity with a full signature (Ben: paragraphs [0008 and 0037]). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of signing a certificate of Ben into the method of Leo in view of Dinker to have a method and system that simplifies the administrative processing associated with the trust paths that are required for valid use of digital certificates (Ben: paragraph [0011]).

Regarding claim 10, this claim has limitations that is similar to those of claims 6, 16 and 21, thus it is rejected with the same rationale applied against claims 6, 16 and 21 above.

Conclusion

11. Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner. In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for

proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2131

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131